INTERNAL CONTROLS ASSESSMENT (ICA)

DEFINITIONS –

INTERNAL CONTROL – an activity, parameter, boundary or action taken by management to mitigate risk and exposure, while increasing the likelihood of achieving established objectives;

CONTROL ENVIRONMENT – often referred to as 'Tone at the Top', involves the setting created by upper management that involves; integrity, values, ethics, and a commitment to competence. It is reflected by the structure of the organization, including the reporting lines through hierarchy, the operational and functional definitions, and the philosophy and style of management;

INTERNAL CONTROL ASSESSMENT – an evaluation of the structure of Internal Control (as defined above), which is management's reaction to risk.

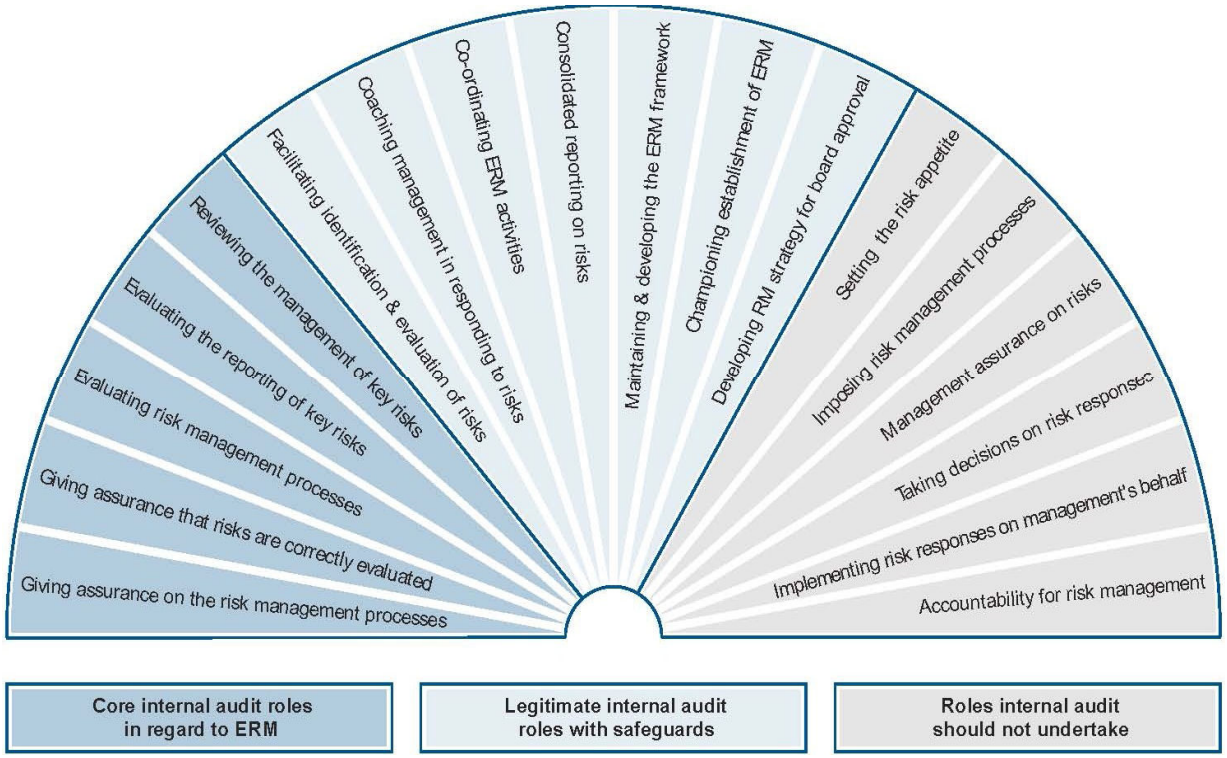
BACKGROUND –

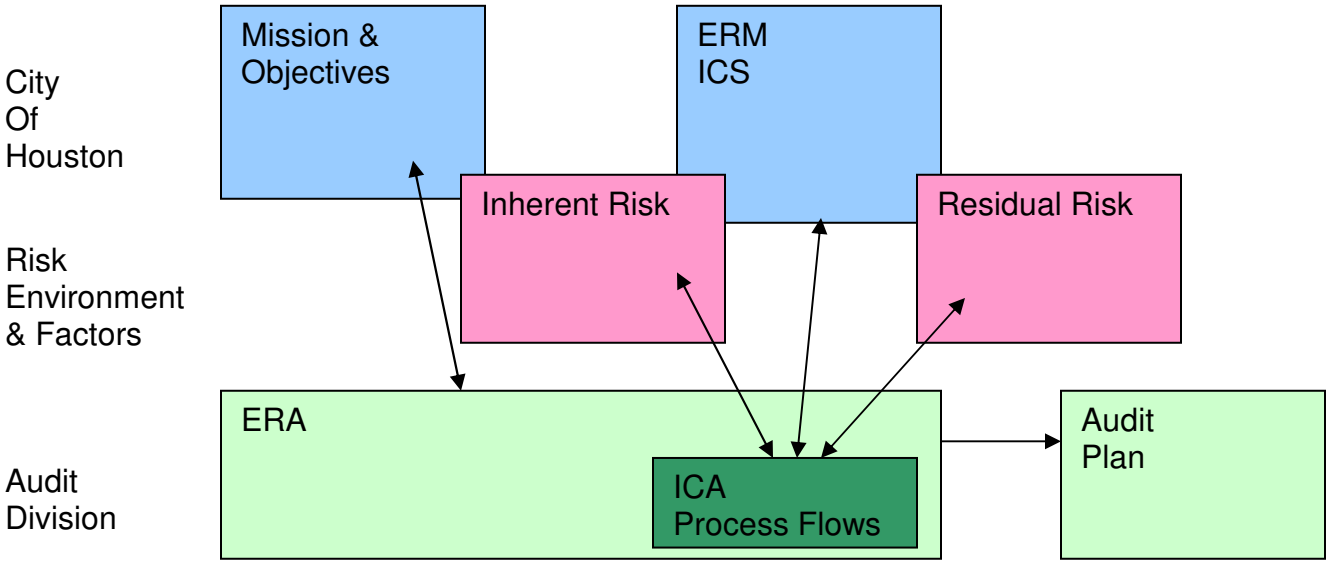
The Internal Control Structure (ICS) is based, in part, on environmental (business and physical), economical, political factors, and management's overall "appetite" for risk or its aversion. The ICS can be designed, created, and monitored using the Committee of Sponsoring Organizations for the Treadway Commission (COSO) framework of Internal Control and ERM. It is management's responsibility to develop this structure as it relates to the entity addressing risk through the creation and application of business, financial, operational, and information processes. This incorporates adequate systems of internal control, sometimes referred to as management control. In the broadest sense, "Internal Control" includes the environment, plans, policies, methods, and procedures adopted by management to meet its missions, goals, objectives and should be interwoven as an integrated function of its ERM.

The AD assumes responsibility to evaluate the adequacy/effectiveness and to make recommendations for the continual improvement of the risk management process. In order to maintain independence and objectivity, internal auditors must not develop the City's ICS; however, it is appropriate for the AD to act in a *consulting* capacity in some of these areas.

As should be clear at this point, internal controls are embedded and interactive with the risk management process and therefore, when looking at internal controls, they are inseparable because they were created to address risk. In fact, the result of the ICA provides information to support conclusions of the ERA and ARA, which then serves as a tool to plan, document, design, and perform subsequent procedures in adapting the specific audit/engagement objectives and audit/engagement program. The formality and depth of the ICA is based on the engagement, but it is always a consideration in planning and performing the necessary procedures to support conclusions.

The chart below is an excerpt from guidance issued by the IIA on ERM and Internal Audit's functional boundaries in relation to that process. The chart is mentioned here because the ICS is a key part of ERM. The boundaries outlined in the chart illustrate an important concept in the AD performing its function.


Reviewing the management of key risks
Evaluating the reporting of key risks
Evaluating risk management processes
Giving assurance that risks are correctly evaluated
Giving assurance on the risk management processes
Facilitating identification & evaluation of risks
Coaching management in responding to risks
Co-ordinating ERM activities
Consolidated reporting on risks
Maintaining & developing the ERM framework
Championing establishment of ERM
Developing RM strategy for board approval
Setting the risk appetite
Imposing risk management processes
Management assurance on risks
Taking decisions on risk responses
Implementing risk responses on management's behalf
Accountability for risk management
Core internal audit roles in regard to ERM
Legitimate internal audit roles with safeguards
Roles internal audit should not undertake


City Of Houston
Risk Environment & Factors
Audit Division
Mission & Objectives
ERM ICS
Inherent Risk
Residual Risk
ERA
ICA Process Flows
Audit Plan

APPROACH AND METHODOLOGY –

Regardless of the level to which the ICA is performed, it is a documented process, and the resulting conclusions are to be included in audit/engagement workpapers. The overall result of the ICA provides support for refining the RA process to identify the residual or unmitigated risk. This process is separated into two major analytical components: *design* and *operation*, as explained below.

DESIGN

Internal Auditors will obtain an understanding of the internal controls that are significant within the context of audit/engagement objectives. Common methods of obtaining an understanding of internal controls include interviews, observations, inspection of documents and records, review of prior audit reports, and direct tests. While obtaining an understanding of program processes and related internal controls, auditors will also determine whether it is necessary to evaluate information system controls. If program processes are not adequately documented, internal auditors will prepare process flow documents/files in which control points will be identified (See section below). The process of assessing the *adequacy* of the design of ICS requires the identification and sufficient understanding of the Control Environment that is significant to the engagement/audit objectives.

OPERATION

ICAs are conducted to determine their *adequacy* and then to determine their *effectiveness*. In order to test the *effectiveness* of Internal Controls, internal auditors will also perform limited testing of each key internal control point identified in program processes (commonly known as a walk-through and usually takes the form of an attribute test). Assessing the Internal Control system for *adequacy* and *effectiveness* is crucial, because it directly relates to the mitigation of risk associated with the achievement of City and Departmental missions, goals and objectives. Assessing Internal Controls also leads to the determination of engagement/audit scope, objectives and methodology (procedures). As a result of ICA, auditors may modify the nature, timing, or extent of procedures.

In the case of performance audits, “an Internal Control deficiency exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions to prevent, detect, or correct (1) impairments to effectiveness or efficiency of operations, (2) misstatements in financial or performance information, or (3) violations of laws and regulations, on a timely basis” (See Yellow Book, Std. 7.21).

Further stated, a deficiency in design exists when (a) a control necessary to meet the control objective is missing or (b) an existing control is not properly designed so that, even if the control operates as designed, the control objective is not met.

A deficiency in operation exists when a properly designed control does not operate as designed, or when the person performing the control does not possess the necessary authority or qualifications to perform the control effectively.

PROCESS FLOWS/DIAGRAMS

In 2009, the AD restructured its organization, which included creating a function for documenting process flows. This function involves identifying key controls within core business/operational processes that have been designed to mitigate the risks inherent to the business purpose and those that are created as a by product of the process design. By mapping processes and identifying the related internal controls, the AD Process Function becomes an integral part of the ICA at both the enterprise (City-Wide) and audit/engagement levels. Because this function is not related specifically to engagement/audit objectives, it provides a more comprehensive understanding of the ICS across the City and serves as a valuable resource for the ERA and the ICA for each audit/engagement.

The ERA process also involves obtaining an understanding of the ICS as it relates to identifying residual risk. Therefore, these functions within the AD are interrelated and interdependent. For example, the ERA identifies operational processes that may not be identified initially through a high-level view of business processes as defined by Enterprise Resource Planning (ERP). Thus, this information becomes vital to the AD Process Function to adequately evaluate key processes on a city-wide basis. Conversely, issues/findings that are identified by the AD Process Function during the course of its work become critical to the ongoing consideration of risk within the City and the continual performance and evolution of the ERA.

Internal auditors will incorporate ICA procedures into audit/engagement programs and will adequately document the results of those assessments in the workpapers. As indicated earlier, the ICA takes the form of a narrative and/or process flow diagram, with control points identified. The workpaper should conclude on the adequacy of the design, while a walk-through should provide support to the conclusion related to the efficiency and effectiveness of the operation and application of the internal controls.

NOTE: Below is a table based on COSO Framework for internal controls and ERM. For each element of the framework there are suggested sources of data to develop and prepare the ICA.

RISK AND INTERNAL CONTROL ASSESSMENT GUIDELINES

	COSO Framework Components		ERM Components
1	Control Environment	1	Internal Environment
		2	Objective Setting
		3	Event Identification
2	Risk Assessment	4	Risk Assessment
		5	Risk Response
3	Control Activities	6	Control Activities
4	Information and Communication	7	Information and Communication
5	Monitoring	8	Monitoring

1	***Control Environment***	
	COSO Framework Elements	**Possible Assessment Methods**
	Integrity and Ethical Values	
	Commitment to Competence	Job descriptions, resumes, retention of competent people, turnover rates/longevity, budget to provide for adequate resources;
	Elected Officials – Mayor, City Council, City Controller	City Council, IA reporting and accountability, governing body, checks and balances;
	Management Philosophy and Operating Style	Department meetings, interview management and others (e.g. receptiveness and openness);
	Organizational Structure	Organizational charts (e.g. Are they well designed and consistent with objectives? etc.);
	Assignment of Authority and Responsibility	Functions operating consistently with organizational chart, perform interviews, etc.;
	Human Resources Policies and Procedures	

2	***Risk Assessment***	
	COSO Framework Elements	**Possible Assessment Methods**
	City-Wide Objectives	City mission statement, policies and procedures, interviews;
	Process-Level Objectives	Policies and procedures, departmental SOPs, departmental missions goals & objectives, interviews, reviewing/documenting process flows;
	Risk Identification and Analysis	Audit Universe (Auditable Entities), interviews to determine engagement risk, identification of audit risk;
	Managing Change	Procedures for maintaining critical documentation and processes, etc.;

3	*Control Activities*	
	COSO Framework Elements	**Possible Assessment Methods**
	Policies and Procedures	Procedures for maintaining current APs, EOs, SOPs, Code of Ordinances, etc.;
	Security (Application and Network)	Security policies and procedures, access limited to only essential personnel, assigned rights, authority, responsibility, and job roles;
	Change Management	Application/Process/Infrastructure change procedures (assess control points), ensure appropriate segregation of duties in the application change process;
	Business Continuity	Assess disaster recovery plan, backup procedures, cross training;
	Outsourcing	Assess adequacy of contract terms and assignment of responsibility;

4	*Information and Communication*	
	COSO Framework Elements	**Possible Assessment Methods**
	Quality of Information	Sample test system data versus source documentation;
	Effectiveness of Communication	Dept./Division/Functional Meetings – notes/minutes;

5	*Monitoring*	
	COSO Framework Elements	**Possible Assessment Methods**
	On-going Monitoring	Existence of monitoring function, adequacy of monitoring procedures, documented results of monitoring activities;
	Separate Evaluation	Are monitoring procedures and results evaluated by independent parties;
	Reporting Deficiencies	Existence of monitoring reports, level to which reports are directed, documentation of the resolution of reported deficiencies;